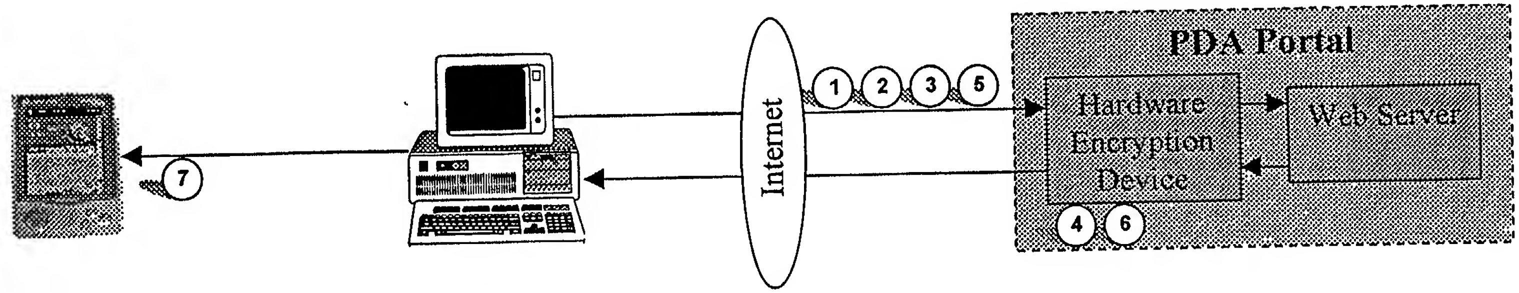
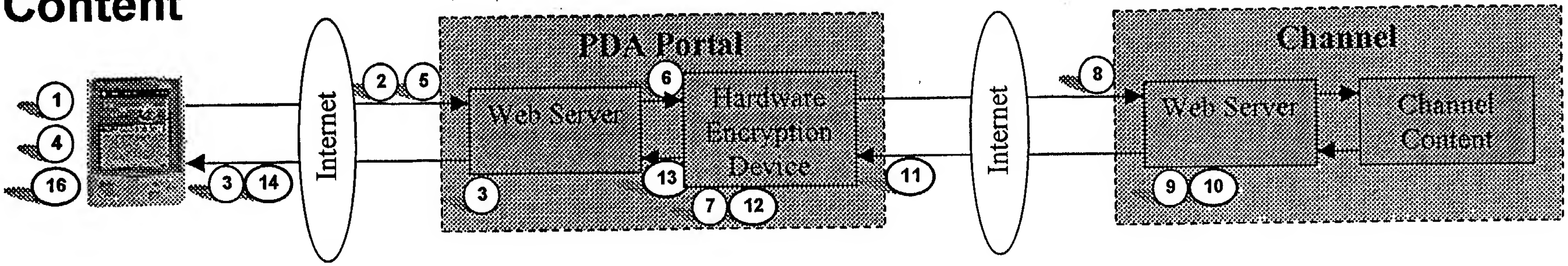
PDA Portal Registration



1. The user goes to the PDA Portal web site from their desktop web browser.
2. The user enrolls in the PDA Portal Service and establishes an account, including selection of channels to be collected during each "sync" request.
3. The "pass-phrase" to be used when accessing secure channels must be entered on a form on the desktop, encrypted using SSL 3.0 and forwarded to the PDA Portal.
4. At the PDA Portal, the hardware encryption device intercepts the response, decrypts the SSL 3.0 "pass-phrase" and stores it on the encryption device. Since the encryption device is secure, there is no need to store it in an encrypted form.
5. For each secure channel that is selected, the user must provide the key information needed to access the pertinent content from that channel (such as an account number). This data is entered onto a form, encrypted using SSL 3.0 following a key exchange with the PDA Portal (the hardware encryption device), and forwarded to the PDA Portal.
6. The hardware encryption device intercepts the request and decrypts the content. The key information is stored on the device in an unencrypted state (since it is a secure device) for that PDA Portal account.
7. Once the setup has completed, the appropriate PDA Portal account and connection information is stored in the user profile at the PDA Portal, and on the PDA.

Figure 1

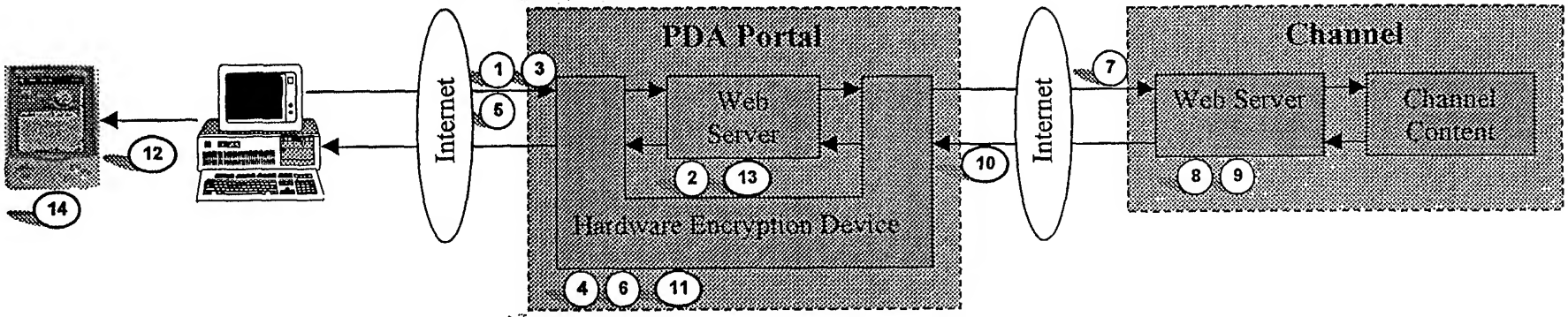
PDA Portal-Establishing Session for Secure Content



1. The user indicates the PDA device is to "sync" with the PDA Portal to refresh the content for their subscribed channels.
2. The PDA connects to the PDA Portal web server.
3. The PDA Portal web server interrogates the channels to be refreshed for the request. If secure content (such as AmEx) is required, the PDA Portal returns to the PDA for the session cookie for each secure channel. If a session cookie does exist, processing continues with step 4 of Channel Updates on the next page.
4. Since the session cookie does not exit, the PDA Portal requests the PDA to prompt the user to enter their user ID and password for that channel (since each channel will have a different user ID/password pair). The user ID and password is encrypted using ECC using "pass-phrase" for the user (which will also need to be entered on the PDA since it is not stored on the device, just the PDA Portal hardware encryption device).
5. The encrypted user ID and password is then returned to the PDA Portal web server.
6. The PDA Portal web server forwards the request to the hardware encryption device.
7. The hardware encryption device decrypts the the user ID and password with ECC and the "pass-phrase" for the user account (which is stored on the device-see PDA Portal Registration). The hardware encryption device then encrypts the request using SSL 3.0 following key exchange with the channel web server.
8. The encrypted session request is then directed to the channel web server.
9. The channel web server decrypts the user ID and password, verifies the user ID/password pair, and establishes a session.
10. The session ID for the session is then encrypted using SSL 3.0 and the negotiated keys.
11. The encrypted session cookie is returned to the PDA Portal hardware encryption device.
12. The hardware encryption device decrypts the SSL 3.0 session cookie, and encrypts it with ECC using the user "pass-phrase" as the key. Additionally, the credentials are hashed with a random number and salted.
13. The encrypted session cookie is returned to the PDA Portal web server.
14. The encrypted session cookie is directed to the PDA and stored on the device (in its encrypted form). As it is received, the device will register which secure channel this cookie is to be used with.
15. Once the session cookie has been established the normal method for refreshing the content for the selected channels is executed (step 4 from the next page).
16. Expiration of the session cookie will be configurable (these types of cookies will not expire every 10 minutes, but could have a duration of several months).

Figure 2

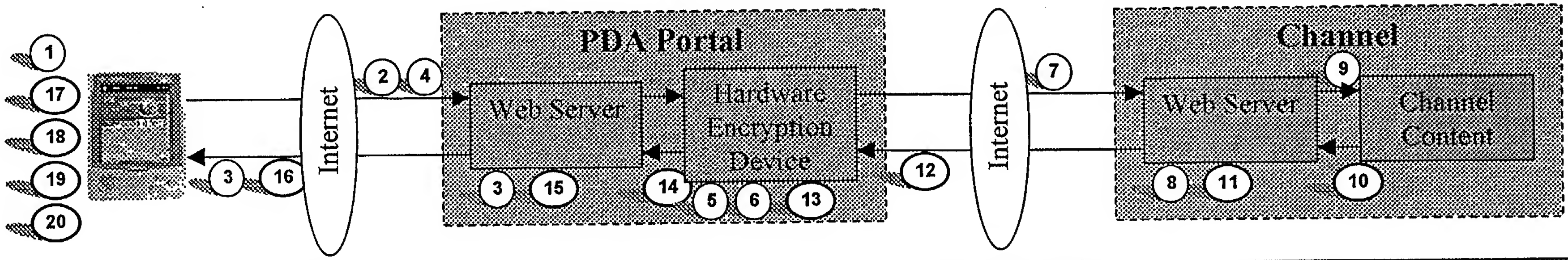
PDA Portal Registration & Establishing Session



1. The user goes to the PDA Portal web site from their desktop web browser.
2. The user enrolls in the PDA Portal Service and establishes an account, including selection of channels to be collected during each "sync" request.
3. The "pass-phrase" to be used when accessing secure channels must be entered on a form on the desktop, encrypted using SSL 3.0 and forwarded to the PDA Portal.
4. At the PDA Portal, the hardware encryption device intercepts the pass-phrase form, decrypts the SSL 3.0 "pass-phrase" and stores it on the encryption device. Since the encryption device is secure, there is no need to store it in an encrypted state.
5. For each secure channel that is selected, the user must provide the key information needed to access the pertinent content from that channel (such as an account number). Additionally, since these channels are secure, each secure channel will require the definition of the user ID and password for accessing the account. This data is entered onto a form and encrypted using SSL 3.0 following a key exchange with PDA Portal (the hardware encryption device).
6. The hardware encryption device intercepts the request and decrypts the content. The key information is stored on the device in an unencrypted state (since it is a secure device) for that PDA Portal account. The user ID and password for the channel is not stored. Instead it is encrypted using SSL 3.0 following a key exchange with the channel web server.
7. The encrypted user ID/password request is forwarded to the channel web server.
8. The channel web server decrypts the user ID and password, verifies the user ID/password pair, and establishes a session.
9. The session ID for the session is then encrypted using SSL 3.0 and the negotiated keys.
10. The encrypted session cookie is returned to the PDA Portal hardware encryption device.
11. The hardware encryption device decrypts the SSL 3.0 session cookie, and encrypts it with ECC using the user "pass-phrase" as the key. Additionally, the credentials are hashed with a random number and salted.
12. The encrypted session cookie is directed to the PDA and stored on the device (in its encrypted form). As it is received, the device will register which secure channel this cookie is to be used with.
13. Once the setup has completed, the appropriate PDA Portal account and connection information is stored in the user profile at PDA Portal, and on the PDA.
14. Expiration of the session cookie will be configurable (these types of cookies will not expire every 10 minutes, but could have a duration of several months).

Figure 3

PDA Portal-Channel Updates



1. The user indicates the PDA device is to "sync" with PDA Portal to refresh the content for their subscribed channels.
2. The PDA connects to the PDA Portal web server.
3. The PDA Portal web server interrogates the channels to be refreshed for the request. If secure content (such as AmEx) is required, the PDA Portal returns to the PDA for the session cookie for each secure channel. If a session cookie does not exist, processing continues with Establishing Session as described on the previous page.
4. The existing session cookie on the PDA is returned to PDA Portal in its encrypted form.
5. The session cookie along with the PDA Portal user account is forwarded to the hardware encryption device. This request does not need to be encrypted as there is no secure content present.
6. The hardware encryption device decrypts the the session cookie using ECC and the "pass-phrase" for the user account (which is stored on the device-see PDA Portal Registration). The key information required to access the desired channel content is combined with the session cookie into a request. The hardware encryption device then encrypts the request using SSL 3.0 following a key exchange with the channel web server.
7. The encrypted request is then forwarded to the channel web server.
8. The channel web server decrypts the encrypted request, and verifies the session ID contained within the cookie.
9. If the session ID is current and valid, the web server passes the key information to the applicable channel content for fulfillment. If the session ID is invalid or expired, an error is returned to PDA Portal and the user is required to re-establish their session cookie (see Establishing Session as described on the previous page).
10. Once the content has been collected, it is returned to the channel web server.
11. The channel web server encrypts the response (referred to as the "payload") using SSL 3.0 using the negotiated keys.
12. The channel web server returns the encrypted response to the hardware encryption device at PDA Portal.
13. The hardware encryption device decrypts the response. It then interrogates the content, removing any links that are present. The remaining content is then encrypted with ECC using the "pass-phrase" that has been established for this user account as the key. The credentials are hashed with a random number and salted.
14. The encrypted content is then passed to the PDA Portal web server.
15. For any links present in the response, the PDA Portal web server will submit additional requests to the channel until all content has been collected (steps 5-13).
16. Once all content (either secure or unsecured) has been collected, it is returned to the PDA and stored.
17. To view the secure content on the PDA, the user will first need to authenticate themselves. This is done by entering their "pass-phrase" which will then be used to decrypt the content and make it available for viewing.
18. Once the content has been decrypted and viewed, the content will be purged from the device memory after a defined period of time (this will be configurable).
19. After entering the "pass-phrase" it will be purged from the device memory after a designated period of time (this will be configurable).
20. If the user removes the channel with secure content or "logs out", the secure content and associated session cookie will be deleted from the device storage.

Figure 4

PDA Portal - Model for Supporting Secure Content - Option 1

OPTIONS:

Two options are provided for consideration. The only real difference between the two is the method for establishing a session for secure channels. In the first option, the identification of the required user ID and password needed to gain access to the secure channel is provided from the PDA. Conversely, the second option requires this process be conducted from the users desktop while the PDA device is connected. While looking at the following pages, option 1 has a registration process that is separate from how a session is created, whereas for option 2, the registration and session creation is integrated.

PRINCIPLES:

1. The PDA Portal web server never has access to the user ID/password or session cookie that is not encrypted.
2. The PDA Portal web server never has access to the "pass-phrase" that is not encrypted.
3. The secure content is visible only on the device after the user has entered their "pass-phrase".
4. The user should not have to provide their user ID/password for each secure channel each time they sync their devices. Therefore, the session for PDA devices will have a different expiration rate than the 10 minutes used for wired Internet use.
5. Establishing sessions with secure channels must be executed from the desktop and not the handheld device. This includes establishing initial, new or renewing expired sessions.
6. No key information will be visible to PDA Portal although it will be housed in the PDA Portal environment. All key information will be stored in the hardware encryption device which itself is secure.
7.
8.
9.
10.

Figure 5

PDA Portal - Model for Supporting Secure Content - Option 2

OPTIONS:

Two options are provided for consideration. The only real difference between the two is the method for establishing a session for secure channels. In the first option, the identification of the required user ID and password needed to gain access to the secure channel is provided from the PDA. Conversely, the second option requires this process be conducted from the users desktop while the PDA device is connected. While looking at the following pages, option 1 has a registration process that is separate from how a session is created, whereas for option 2, the registration and session creation is integrated.

PRINCIPLES:

1. The PDA Portal web server never has access to the user ID/password or session cookie that is not encrypted.
2. The PDA Portal web server never has access to the "pass-phrase" that is not encrypted.
3. The secure content is visible only on the device after the user has entered their "pass-phrase".
4. The user should not have to provide their user ID/password for each secure channel, each time they sync their devices. Therefore, the session for PDA devices will have a different expiration rule than the 10 minutes used for wired Internet use.
5. Establishing sessions with secure channels must be executed from the desktop and not the handheld device. This includes establishing initial, new or renewing expired sessions.
6. No key information will be visible to PDA Portal although it will be housed in the PDA Portal environment. All key information will be stored in the hardware encryption device which itself is secure.
7.
8.
9.
10.

Figure 6